THÈSE

DE DOCTORAT DE TROISIEME CYCLE DE MATHÉMATIQUES PURES

présentée

A L'UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE

DE GRENOBLE

par

Roland GILLARD

SUR LE PROBLEME DU PLONGEMENT DES EXTENSIONS GALOISIENNES

Soutenue le 23 février 1973 devant la Commission d'examen

C. CHABAUTY Président

J.M. FONTAINE
J.J. PAYAN
G. POITOU
Examinateurs

THÈSE

DE DOCTORAT DE TROISIÈME CYCLE DE MATHÉMATIQUES PURES

présentée

A L'UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE
DE GRENOBLE

par

Roland GILLARD

SUR LE PROBLEME DU PLONGEMENT DES EXTENSIONS GALOISIENNES

Soutenue le 23 février 1973 devant la Commission d'examen

C. CHABAUTY Président

J.M. FONTAINE
J.J. PAYAN Examinateurs
G. POITOU

UNIV.
LEIDEN
BIBL.

Je suis particulièrement reconnaissant à Monsieur C. CHABAUTY d'avoir accepté de présider ce jury. Je lui dois d'avoir pu travailler à Grenoble dans les meilleures conditions.

Que Monsieur G. POITOU qui m'a initié à la théorie des nombres et qui m'a donné l'idée de ce travail trouve ici l'expression de ma profonde gratitude.

Je dois beaucoup à Monsieur J.J. PAYAN qui s'est constamment intéressé à ce travail. Monsieur J.M. FONTAINE a aussi accepté de faire partie de ce jury, je l'en remercie vivement.

Madame GUTTIN-LOMBARD, Messieurs GAUDE et GIRARD ont apporté beaucoup de soin et de gentillesse à la réalisation matérielle de ce travail. Je les en remercie chaleureusement

SOMMAIRE

Pages

Chapitre I. THEORIE GENERALE 1

1. Introduction 1
2. Traduction cohomologique 1
3. Localisation du problème 4
4. Etude des conditions locales 5

Chapitre II. PLONGEMENT DANS UNE SUREXTENSION ABELIENNE 8

1. Première réduction 8
2. Réduction au cas où E est cyclique primaire..... 8
3. Etude du cas où E est cyclique primaire 10

Chapitre III. PLONGEMENT D'UNE EXTENSION QUADRATIQUE DANS UNE EXTENSION QUATERNIONIENNE..... 14

1. Introduction, énoncé des résultats..... 14
2. Etude de la condition sur les places infinies..... 16
3. Places modérément ramifiées dans K/k..... 17
4. Etude pour (P_2) 17
5. Etude pour (P_4) 18
6. Etude pour (P_8) 19
7. Cas où le corps k est celui des rationnels 22

Chapitre IV. PLONGEMENT DANS UNE SUREXTENSION DE DEGRE P^3 . 24

1. Introduction 24
2. Examen des données 24
3. Localisation de la condition de plongement..... 26
4. "Oubli" d'une place 31
5. Récapitulation ($p \neq 2$) 33
6. Etude pour p = 2 et k = $\mathbb{Q}$; comparaison avec [4] et [7] 34

BIBLIOGRAPHIE 38

INTRODUCTION

Il est naturel de se demander si un corps de nombres k admet une extension de groupe de Galois donné (cf. [12] et [14]). On peut aussi se demander si, connaissant une extension K/k de groupe de Galois G, et un groupe E dont G est un quotient, il existe une surextension N/k contenant K, de groupe de Galois isomorphe à E et telle que la restriction des automorphismes corresponde au passage au quotient $E \to G$. C'est le problème du plongement (cf. [1], [5], [7], [8], [9], [13], [15] et [19]). Il existe essentiellement deux méthodes d'approche.

L'une utilise la théorie de Kummer : soient k' et K' les corps de nombres obtenus en rajoutant à k et K suffisamment de racines de l'unité, on cherche à construire une extension de Kummer N' de k' de groupe de Galois E et décomposée sur k. C'est le point de vue de [4], [5], [9]. L'article [10] y joue un rôle essentiel.

L'autre méthode [8], utilisée ici, consiste à interpréter E comme extension de G par un sous-groupe A (cf. [2] chap. XIII). Lorsque A est abélien cette extension est décrite par une structure de G module sur A (issue de la conjugaison dans E) et un élément ε du groupe de cohomologie $H^2(G,A)$. Soient $\bar{k}$ une clôture algébrique de k et $\bar{G}$ son groupe de Galois : on est ramené à l'étude de la nullité d'un élément $\bar{\varepsilon}$ de $H^2(\bar{G},A)$ (cf. th. 1 du chap. I). L'étude d'un problème de plongement par cette méthode se divise alors en deux étapes : on cherche si on peut se ramener à des conditions locales (cf. chap. I th. 2) puis on explicite ces conditions (chap. I th. 3 et 4).

La théorie générale est décrite dans le chapitre I. Son illustration fait l'objet des chapitres suivants. Ceux-ci sont indépendants entre eux.

Dans le chapitre II, on étudie le problème de plongement des extensions abéliennes dans des surextensions abéliennes. Des théorèmes de réduction permettent de se ramener au cas des extensions cycliques. On retrouve alors un résultat classique (th. 1 et th. 2, cf. [2] et [13]) obtenu en général dans la littérature par la théorie du corps de classes.

Dans le chapitre III, on s'intéresse aux extensions quaternioniennes généralisées. Soit K/k une extension quadratique. Soit n un nombre pair non nul et soit E le groupe d'ordre $2n$ défini par deux générateurs σ et τ vérifiant les relations :

$$\sigma^n = 1$$

$$\tau^2 = \sigma^{n/2}$$

$$\tau\sigma\tau^{-1} = \sigma^{-1} .$$

Soit A le sous-groupe cyclique distingué engendré par σ et soit G le quotient. Ce groupe, d'ordre 2, s'identifie au groupe de Galois de K/k. Pour le problème de plongement ainsi défini on voit immédiatement (th. 1) que l'on peut supposer que E est un 2-groupe : on est ramené au problème de [5]. Les théorèmes 2 et 3 résument nos résultats. On notera que la méthode employée est limitée par le fait que la réduction aux conditions locales n'est pas toujours valable.

On remarque que l'hypothèse que K/k soit cyclique simplifie considérablement les conditions locales (cf. chap. II et III) : au chapitre IV on se place dans le cas le plus simple sortant de ce cadre : soit p un nombre premier, on suppose que K/k est une extension galoisienne de type (p,p). Soit E le groupe d'ordre p^3 à deux générateurs σ et τ vérifiant les relations :

$$\sigma^{p^2} = 1$$

$$\tau^p = 1$$

$$\tau\sigma\tau^{-1} = \sigma^{1+p} .$$

Soit A le sous-groupe cyclique engendré par σ^p et G le quotient identifié

non canoniquement au groupe de Galois de K/k . On s'aperçoit que le problème de plongement se ramène toujours à la vérification des conditions locales (cf. th. 1). Lorsque G_v est d'ordre p les conditions locales s'explicitent sans trop de mal, les méthodes mises en jeu aux chapitres II et III s'appliquant encore. Par contre, lorsque G_v est d'ordre p^2 on doit chercher autre chose : notre méthode consiste à interpréter la condition locale en termes de problème de plongement de corps locaux. Pour les places premières à p ce problème se résoud à l'aide de la théorie de Kummer. Pour les places au-dessus de p la situation est bien plus compliquée : on tourne la difficulté en montrant qu'on peut "oublier" une place dans certains cas. Ceci permet de donner un énoncé qui contient complètement le cas $k = \mathbb{Q}$ (théorème 2 pour $p \neq 2$ et théorème 3 pour $p = 2$).

CHAPITRE I

THEORIE GENERALE

I.1. Introduction.

Rappelons tout d'abord la définition du problème du plongement. On se donne une extension galoisienne K/k de corps commutatifs, de groupe de Galois G. On se donne aussi une suite exacte de groupes :

$$1 \to A \to E \to G \to 1$$

On appelle solution au problème de plongement (P) une surextension galoisienne N de k telle qu'il existe un isomorphisme π, induisant π' sur A rendant le diagramme suivant commutatif :

$$\begin{array}{ccccccc} 1 \to & A & \to & E & \to & G & \to 1 \\ & \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} & & \downarrow & \\ 1 \to & G(N/K) & \to & G(N/k) & \to & G(K/k) & \to 1 \end{array}$$

On supposera dans toute la suite que E est fini, A étant un sous-groupe abélien.

I.2. Traduction cohomologique.

La suite exacte de groupes de I.1 sera décrite (à isomorphisme près) cf. [2] chap. XIII, par la structure correspondante de G-module sur A et un élément ε de $H^2(G,A)$, cet élément n'étant nul que si la suite exacte est scindée, E étant alors extension décomposée de A par G.

Soit $\bar{k}$ une clôture algébrique de k, $\bar{G}$ le groupe de Galois de

$\bar{k}/k$. Si (P) admet une solution N , on a un diagramme commutatif d'homomorphismes surjectifs des groupes de Galois :

$$\begin{array}{ccc} & & \bar{G} \\ & \swarrow & \downarrow \\ G(N/k) & \longrightarrow & G \\ \downarrow & & \downarrow \\ E & \longrightarrow & G \end{array}$$

Il existe donc un homomorphisme surjectif Φ rendant le diagramme suivant commutatif :

$$\begin{array}{ccc} & & \bar{G} \\ & \overset{\Phi}{\swarrow} & \downarrow \\ E & \longrightarrow & G \end{array} \qquad (D) \ .$$

Réciproquement, si un tel Φ existe en prenant pour N le corps associé à son noyau, on obtient une solution à (P) . A l'aide de [8] 2.3 et 6.7, on peut supprimer l'hypothèse de surjectivité dans les cas suivants :

Lemme 1.

Lorsque K/k est une extension de corps de nombres algébriques ou lorsque G et E sont des p-groupes de même rang, l'existence d'un homomorphisme Φ rendant (D) commutatif entraîne celle d'un homomorphisme surjectif ayant la même propriété.

Considérons le diagramme suivant :

$$\begin{array}{ccccccccc} 1 & \to & A & \to & E \times_G \bar{G} & \overset{p_2}{\to} & \bar{G} & \to & 1 \\ & & \downarrow & & \downarrow p_1 & & \downarrow & & \\ 1 & \to & A & \to & E & \to & G & \to & 1 \end{array} \qquad (D_1) \ .$$

Ici $E \times_G \bar{G}$ désigne le sous-ensemble de $E \times \bar{G}$ des couples (e,g) formé d'éléments qui ont même image dans G . Les applications p_1 et p_2 sont les projections. On voit facilement que le diagramme ci-dessus est commutatif et que sa première ligne est aussi exacte. L'opération de $\bar{G}$ sur A correspondante se fait par l'intermédiaire de G . L'élément de $H^2(\bar{G},A)$ qui caractérise cette extension n'est autre que inf ε , image de ε par inflation.

On peut alors énoncer :

Théorème 1.

Dans les hypothèses du lemme 1, pour que (P) admette une solution, il faut et il suffit que l'image de ε par l'inflation suivante soit nulle :

$$H^2(G,A) \to H^2(\bar{G},A) .$$

Démonstration :

Si on a un homomorphisme Φ complétant (D), l'application $\Phi \times Id$ de $\bar{G}$ dans $E \times \bar{G}$ définit une section linéaire pour la suite exacte de la première ligne de (D_1) qui est donc scindée ; l'élément inf ε qui la représente dans $H^2(\bar{G},A)$ est donc nul. Réciproquement, si inf ε est nul, la suite est scindée, soit s une section linéaire, il est bien clair que $p_1 \circ s$ rend (D) commutatif.

Corollaire 1.

Si E est extension décomposée de A par G, (P) admet toujours une solution dans les hypothèses du lemme 1.

Corollaire 2.

K/k étant ici une extension de corps de nombres, on suppose que le groupe A se décompose en somme directe de G-modules A_i $(i = 1...r)$. Le problème de plongement relatif à une extension E de A par G admet une solution si et seulement si il en est de même des problèmes relatifs à des extensions E_i des A_i par G.

Démonstration :

Pour le corollaire 1, il suffit de remarquer que si ε est nul, inf ε aussi. Pour le corollaire 2, on observe qu'à la décomposition $A = \bigoplus_{i=1}^{r} A_i$ correspond les décompositions $H^2(G,A) = \bigoplus_{i=1}^{r} H^2(G,A_i)$ et : $H^2(\bar{G},A) = \bigoplus_{i=1}^{r} H^2(\bar{G},A_i)$.

On a donc $\inf \varepsilon = \oplus \inf \varepsilon_i$. La nullité de $\inf \varepsilon$ est équivalente à celle des $\inf \varepsilon_i$. Or si ε_i correspond à l'extension E_i de A_i par G la nullité de $\inf \varepsilon_i$ s'interprète sous forme d'un problème de plongement.

I.3. Localisation du problème.

On suppose que K/k est une extension de corps de nombres. On introduit alors les notations suivantes : soient n l'ordre de A , ζ une racine primitive $n^{\text{ième}}$ de l'unité, K' le corps $K(\zeta)$ et Γ' son groupe de Galois sur k . Soit $\hat{A}$ le groupe $\mathrm{Hom}(A,\bar{k}^*)$, les groupes $\bar{G}$ et Γ' opérant sur $\hat{A}$ par $(\sigma\chi)(a) = \sigma\chi(\sigma^{-1}a)$ pour tout χ de $\hat{A}$, tout a de A et tout σ dans Γ' ou $\bar{G}$. Pour chaque place v finie ou non de k , on choisit un prolongement, noté aussi v , à $\bar{k}$, correspondant à des groupes de décomposition G_v , Γ'_v , $\bar{G}_v$ et à des complétés k_v , K_v , K'_v . On désigne aussi par $\bar{k}_v$ une clôture algébrique de K'_v . Soit L le sous-corps de K' associé au sous-groupe de Γ' laissant fixes les éléments de $\hat{A}$. On note par Γ son groupe de Galois sur k , et Γ_v le groupe de décomposition correspondant. Enfin, on désigne par $\hat{A}_v$ le sous-groupe des caractères invariants par Γ'_v .

L'idée de la méthode est d'utiliser l'application h suivante, produit de restrictions dont on peut discuter l'injectivité à l'aide des théorèmes de dualité globale de Poitou et Tate (cf. [11]).

$$H^2(\bar{G},A) \xrightarrow{h} \prod_v H^2(\bar{G}_v,A) \quad .$$

Le théorème 6.3 de [8] donne le résultat suivant :

Théorème 2.

Pour que h soit injective, il suffit que les indices $[\Gamma:\Gamma_v]$ soient premiers entre eux dans leur ensemble (ce qui est vérifié notamment dans le cas où Γ est cyclique). La condition est nécessaire si A est un p-groupe cyclique.

I.4. Etude des conditions locales.

L'étude de $h(\inf \varepsilon)$, motivée par le théorème 2, peut se faire à l'aide du joli diagramme suivant :

$$\begin{array}{ccccccc} H^2(G,A) & \longrightarrow & \prod_v H^2(G_v,A) & \longrightarrow & \prod_v H^2(\Gamma'_v,A) & \longrightarrow & \prod_{v,\chi} H^2(\Gamma'_v,K'^*_v) \\ \downarrow & & \searrow \quad \swarrow & & & & \downarrow \\ H^2(\bar{G},A) & \xrightarrow{h} & \prod_v H^2(\bar{G}_v,A) & \longrightarrow & & & \prod_{v,\chi} H^2(\bar{G}_v,\bar{k}^*_v) \end{array}$$

On passe de la première ligne à la seconde par des inflations. Les premières applications de chaque ligne sont des produits de restrictions. Elles forment avec les inflations un diagramme commutatif résultant des diagrammes :

$$\begin{array}{ccc} \bar{G}_v & \longrightarrow & \bar{G} \\ \downarrow & & \downarrow \\ G_v & \longrightarrow & G \end{array} \quad .$$

Le triangle central est défini par des produits d'inflations. La commutativité provient de celle du diagramme :

$$\begin{array}{ccc} \bar{G}_v & \longrightarrow & \Gamma'_v \\ & \searrow & \downarrow \\ & & G_v \end{array} \quad .$$

La dernière application de chaque ligne est définie pour le facteur correspondant à v par le produit des caractères dans $\hat{A}_v$. La commutativité résulte ici des propriétés de l'inflation. D'après le théorème de dualité locale de Tate, la dernière application de la seconde ligne est injective (cf. par exemple [11]) ; comme la dernière colonne est injective (cf. [17] X, §5 cor. de prop. 5), la nullité de $h(\inf \varepsilon)$ est équivalente à celle de l'image de ε par l'application de la première ligne. Introduisons donc pour chaque place v et chaque caractère χ dans $\hat{A}_v$ l'application :

$$\wedge_{v,\chi} : H^2(G,A) \xrightarrow{\text{res}} H^2(G_v,A) \xrightarrow{\text{inf}} H^2(\Gamma'_v,A) \xrightarrow{H^2(\chi)} H^2(\Gamma'_v,K'^*_v) \ .$$

On peut alors énoncer :

Théorème 3.

Si (P) admet une solution, l'image de ε par $\wedge_{v,\chi}$ est nulle pour toute place v de k et tout caractère χ dans $\hat{A}_v$. La réciproque est vraie si h est injective (cf. par exemple théorème 2).

On appellera condition locale en v la condition d'annulation des $\wedge_{v,\chi}(\varepsilon)$ pour tout $\chi \in \hat{A}_v$.

En fait seul un nombre fini de places fait problème :

Théorème 4.

Si v est non ramifiée dans K'/k , $\wedge_{v,\chi}$ est nulle pour tout χ dans $\hat{A}_v$. Il en est de même si v est totalement décomposée dans K/k .

Démonstration :

Si v est ramifiée dans K'/k , Γ'_v est cyclique. La dernière application entrant dans la définition de $\wedge_{v,\chi}$ peut s'étudier à l'aide de la cohomologie modifiée d'indice nul :

$$A^{\Gamma'_v}/NA \simeq \hat{H}^0(\Gamma'_v, A) \to \hat{H}^0(\Gamma'_v, K'^*_v) \simeq k^*_v/N_{K'_v/k_v}(K'^*_v) \quad .$$

Cette application est donc induite par χ :

$$A^{\Gamma'_v} \xrightarrow{\chi} k^*_v \longrightarrow k^*_v/NK'^*_v \quad .$$

Or, l'image de χ est constituée de racines de l'unité donc d'unités de k_v donc de normes de K'_v (toujours à cause de l'absence de ramification). L'application $\wedge_{v,\chi}$ est donc nulle.

Si la place v est totalement décomposée dans K/k, G_v est nul. Donc l'application $\wedge_{v,\chi}$ est nulle .

Remarque :

Soit ε_v la restriction de ε dans $H^2(G_v, A)$. On sait que ε_v correspond à la suite exacte (E_v est l'image réciproque de G_v dans E) :

$$1 \to A \to E_v \to G_v \to 1 \quad .$$

On a donc un problème de plongement local avec K_v/k_v et ε_v . On peut remarquer que la condition d'annulation des $\wedge_{v,\chi}(\varepsilon)$ provient en fait de l'annulation de $\inf \varepsilon_v$ dans $H^2(\bar{G}_v, A)$. Autrement dit, si les conclusions du lemme 1 sont vérifiées pour le problème local de plongement, celui-ci admet une solution si, et seulement si, notre condition locale sur les $\wedge_{v,\chi}$ est vérifiée. Cette remarque sera utile pour simplifier les conditions locales dans les cas des chapitres II et IV .

CHAPITRE II

PLONGEMENT DANS UNE SUREXTENSION ABELIENNE

Dans ce chapitre, on reprend les notations du chapitre I , E étant ici un groupe commutatif, K/k étant une extension de corps de nombres. On dira qu'un groupe est primaire si son ordre est une puissance d'un nombre premier. Comme Richter [13] on réduit le problème au cas où E est cyclique primaire.

II.1. Première réduction.

Le groupe A , étant abélien, peut se représenter comme somme directe de groupes (donc de G-modules, puisque G agit ici trivialement) cycliques primaires :

$$A = \bigoplus_{i=1}^{I} A_i \quad .$$

On utilise alors le corollaire 2 de I. théorème 1, pour se ramener à des problèmes de plongement relatifs à des extensions de A_i par G .

Ceci montre que pour la suite on peut se limiter au cas où A est un groupe cyclique primaire.

II.2. Réduction au cas où E est cyclique primaire.

Comme E est abélien on peut le représenter par une somme directe de groupes cycliques primaires :

$$E = \bigoplus_{i=1}^{r} E_i \quad .$$

On note a_i un générateur de E_i $(i=1,\ldots,r)$. Supposant A cyclique primaire, un de ses générateurs peut s'écrire :

$$a = \sum_{i=1}^{r} x_i a_i \quad , \quad x_i \in \mathbb{N} \quad \text{pour} \quad i = 1,\ldots,r \ .$$

Soit $n = \ell^\nu$ l'ordre de A , une des composantes au moins de a est d'ordre ℓ^ν soit par exemple $a_1 x_1$. On pose alors :

$$H = A \oplus H' \quad \text{avec} \quad H' = E_2 \oplus \ldots \oplus E_r \ .$$

Soit $\overline{H}$ l'image de H dans G . On note alors :

$$G_1 = E/H \simeq G/\overline{H} \ .$$

La suite exacte :

$$1 \to H/H' \to E/H' \to E/H \to 1$$

se traduit donc par la suite exacte :

$$1 \to A \to E_1 \to G_1 \to 1 \ .$$

On désigne par K_1 le sous-corps de K associé à $\overline{H}$ et par (P_1) le problème de plongement relatif à K_1/k et à E_1 considéré comme extension de A par G_1 . On peut alors énoncer la proposition suivante qui établit la possibilité de se ramener au cas où E est cyclique primaire :

Proposition 1.

Pour que le problème (P) admette une solution, il faut et il suffit qu'il en soit de même pour (P_1) .

Démonstration :

On a le diagramme commutatif suivant reliant nos deux suites exactes :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & E_1 & \longrightarrow & G_1 & \longrightarrow & 1 \end{array} \ .$$

Il en résulte que ε est l'image par inflation de ε_1 , représentant de la deuxième ligne dans $H^2(G_1,A)$. Si on considère le diagramme :

$$\begin{array}{ccc} H^2(G_1,A) & \xrightarrow{\inf} & H^2(G,A) \\ & \searrow^{\inf} & \downarrow \inf \\ & & H^2(\bar{G},A) \end{array} .$$

On voit que les images de ε et ε_1 par inflation dans $H^2(\bar{G},A)$ sont nulles en même temps, d'où la proposition d'après le théorème 1 de I.2.

II.3. Etude du cas où E est cyclique primaire.

Soient donc $n = \ell^\nu$ et $m = \ell^\mu$ les ordres de A et G . Le groupe E étant abélien, A est un G-module trivial ; $\bar{G}$ opère donc sur $\hat{A}$ par action galoisienne sur les racines de l'unité. On aura donc $L = k(\zeta)$ en reprenant les notations de I .

a) Etude de l'injectivité de h .

Elle se fait à l'aide de I.3., théorème 2 : si ℓ est impair, L est cyclique sur k , et h est injective. Si ℓ est égal à 2 et L cyclique, on conclut de la même façon. Si L n'est pas cyclique, h est injective si et seulement s'il existe une place v telle que $[\Gamma:\Gamma_v] = 1$. La place v doit donc être non décomposée dans L , ou ce qui revient au même dans la sous-extension bicyclique biquadratique de L . Si v ne divise pas 2 , v est non ramifiée dans L donc Γ_v est cyclique donc a priori distinct de Γ . Tout ceci permet d'énoncer :

Proposition 2.

L'application h est injective si et seulement si $k(\zeta)$ est cyclique sur k ou, n'étant pas cyclique, possède une place (nécessairement au-dessus de 2) non décomposée dans la sous-extension biquadratique bicyclique de $k(\zeta)/k$.

b) Etude des conditions locales.

Lemme 1.

Si E , extension de A par G , est cyclique primaire, l'élément ε associé est un générateur de $H^2(G,A)$.

Démonstration :

Soit ℓ^{α} le cardinal de $H^2(G,A)$, remarquons que ℓ^{α} est inférieur ou égal à ℓ^{μ} , ordre de G . Il s'agit de vérifier que $\ell^{\alpha-1}\varepsilon$ $(\alpha>0)$ est non nul. Soit H le sous-groupe de G d'indice $\ell^{\alpha-1}$, $\ell^{\alpha-1}\varepsilon$ n'est autre que l'image de ε par l'application :

$$H^2(G,A) \xrightarrow{\text{res}} H^2(H,A) \xrightarrow{\text{cor}} H^2(G,A) \quad .$$

Mais res ε représente en fait l'extension définie par la suite exacte suivante (E' image réciproque de H dans E) :

$$I \to A \to E' \to H \to 1 \ .$$

Or, E' étant cyclique cette extension n'est pas décomposée : res $\varepsilon \neq 0$. Vérifions maintenant que la corestriction est injective :

$$\begin{array}{ccc} H^2(H,A) & \xrightarrow{\text{cor}} & H^2(G,A) \\ \downarrow{\scriptstyle k} & & \downarrow{\scriptstyle k} \\ A^H/[H].A & \xrightarrow{\text{cor}} & A^G/[G].A \end{array} \quad .$$

On a noté $[H]$ et $[G]$ les ordres des groupes H et G . La corestriction s'interprète en cohomologie modifiée d'ordre 0 comme la norme de G/H , donc ici par la multiplication par $\ell^{\alpha-1}$:

$$A/\ell^{\mu-\alpha+1} \to A/\ell^{\mu} \quad .$$

La corestriction est donc injective : cor $\circ$ res $\varepsilon \neq 0$.

L'intérêt du lemme 1 est de se ramener à l'étude de la nullité des applications $\wedge_{v,\chi}$, sans référence à ε :

$$\wedge_{v,\chi} : H^2(G,A) \xrightarrow{\text{res}} H^2(G_v,A) \xrightarrow{\text{inf}} H^2(\Gamma'_v,A) \xrightarrow{H^2(\chi)} H^2(\Gamma'_v,K'^{*}_v) \quad .$$

Les seuls caractères à considérer sont ceux de $\hat{A}_v$, invariants par Γ'_v . Or, dire que χ est invariant par Γ'_v revient à dire que son image $\chi(A)$ est dans k_v . On peut donc calculer $\wedge_{v,\chi}$ à l'aide du diagramme commutatif dont la dernière colonne est une inflation injective :

$$\begin{array}{ccccc} H^2(G,A) & \xrightarrow{\text{res}} & H^2(G_v,A) & \xrightarrow{H^2(\chi)} & H^2(G_v,K_v^*) \\ & & \downarrow \text{inf} & & \downarrow \text{inf} \\ & & H^2(\Gamma'_v,A) & \xrightarrow{H^2(\chi)} & H^2(\Gamma'_v,K_v'^*) \end{array} .$$

Comme res ε d'après le lemme 1 engendre $H^2(G_v,A)$ la nullité de $\wedge_{v,\chi}(\varepsilon)$ est équivalente à celle de l'application $H^2(\chi)$:

$$H^2(G_v,A) \rightarrow H^2(G_v,K_v^*) .$$

Cette application peut s'étudier (G_v étant cyclique) à l'aide de l'application :

$$A/[G_v].A \simeq \hat{H}^\circ(G_v,A) \xrightarrow{\chi} \hat{H}^\circ(G_v,K_v^*) \simeq k_v^*/NK_v^* .$$

$\wedge_{v,\chi}$ est nulle si, et seulement si, $\chi(A)$ est inclus dans NK_v^* groupe des normes de K_v^* dans k_v^*, ceci devant être vrai pour tout caractère χ invariant par Γ'_v.

Proposition 3.

$\wedge_{v,\chi}(\varepsilon)$ est nul pour tout χ de $\hat{A}_v$ si et seulement si toutes les racines $n^{\text{ièmes}}$ de l'unité qui sont dans k_v^* sont des normes de K_v^*.

Démonstration :

Elle résulte du fait que toutes les racines $n^{\text{ièmes}}$ de l'unité qui sont dans k_v correspondent à des caractères invariants et réciproquement.

On peut donc énoncer le théorème suivant (cf. [13] et aussi [2] chap. X) :

Théorème 1.

E étant supposé cyclique primaire, si (P) admet une solution alors pour chaque place v de k, les racines $n^{\text{ièmes}}$ de l'unité qui sont dans k_v sont des normes de K_v. Cette condition est suffisante si $k(\zeta)/k$ est cyclique, ou sinon, quand sa sous-extension biquadratique bicyclique possède une place au moins (divisant forcément 2) non décomposée sur k.

c) Autre énoncé des conditions locales pour les places modérément ramifiées.

Soit v une place finie ramifiée modérément avec l'indice e ($e>1$) . On va exprimer autrement la condition locale : G_v et E_v étant de même rang (cf. pour les notations fin de I.4.) la condition locale se réduit en fait à un problème de plongement local : une solution de ce problème est une extension cyclique de k_v . On voit alors que nécessairement son indice de ramification est $(e.n)$. L'existence d'une telle solution implique donc que k_v contienne les racines de l'unité d'ordre $(e.n)$ (cf. [3] chap. VI 2.5 corollaire, chap. I 8 prop. 2 et chap. II appendice C lemme).

Réciproquement, si k_v contient les racines de l'unité d'ordre $(e.n)$, ce sont des normes de la sous-extension non ramifiée maximale de K_v et les racines $n^{\text{ièmes}}$ sont des normes de K_v : la condition locale du b) est remplie ; ainsi on a une condition équivalente :

Proposition 4.

Si v est une place de k , ramifiée modérément avec l'indice e ($e>1$) dans K , pour que les applications $\wedge_{v,\chi}$ pour χ dans $\hat{A}_v$ soient nulles, il faut et il suffit que k_v contienne les racines de l'unité d'ordre $(e.n)$.

Donnons une conséquence de cette proposition : lorsque k est le corps des rationnels en utilisant la proposition 3 pour les places infinies et celle au-dessus de ℓ et la proposition 4 dans les autres cas, on obtient immédiatement le théorème suivant (cf. [13]) :

Théorème 2.

Pour qu'une extension cyclique de degré ℓ^μ de $\mathbb{Q}$ se plonge dans une extension cyclique de degré $\ell^{\mu+\nu}$ il faut qu'elle soit totalement réelle et que tout nombre premier q différent de ℓ , ramifié avec l'indice e ($e>1$) vérifie la congruence :

$$q \equiv 1 \bmod (e\ell^\nu) .$$

La condition de réciproque est la même que pour le théorème 1.

CHAPITRE III

PLONGEMENT D'UNE EXTENSION QUADRATIQUE DANS UNE EXTENSION QUATERNIONIENNE.

III.1. Introduction.

Dans ce chapitre, on appelle groupe quaternionien généralisé, le groupe E_n d'ordre $2n$ (n étant un nombre pair strictement positif) engendré par deux éléments σ et τ vérifiant les relations :

$$\sigma^n = 1$$

$$\tau^2 = \sigma^{n/2}$$

$$\tau\sigma\tau^{-1} = \sigma^{-1} \quad .$$

Soit A_n le sous-groupe engendré par σ et $G = \{1, \bar{\tau}\}$, le quotient. G opère donc par symétrie sur A_n. L'extension de A_n par G est non décomposée, l'élément ε_n associé dans $H^2(G,A_n)$ n'est donc pas nul. Calculons $H^2(G,A_n)$:

$$H^2(G,A_n) \simeq \hat{H}^0(G,A_n) \simeq A_n^G/NA_n \simeq \{1,\sigma^{n/2}\} \quad .$$

On considère une extension quadratique de corps de nombres K/k, avec $K = k(\sqrt{\alpha})$ où α est un entier de k n'appartenant pas à $(k^*)^2$. On identifie le groupe de Galois de K/k à G. On note (P_n) le problème de plongement relatif à E_n. Le théorème suivant permet de comparer les problèmes relatifs à deux indices :

Théorème 1.

Si (P_n) admet une solution, il en est de même de $(P_{n'})$ pour tout n' multiple de n . La réciproque est vraie si n'/n est impair lorsque n est une puissance de 2 .

Démonstration :

En envoyant un générateur de A_n sur une puissance (n'/n) d'un générateur de $A_{n'}$, on obtient un G-homomorphisme injectif $A_n \to A_{n'}$ qui induit un isomorphisme sur les groupes $\hat{H}^\circ$ donc aussi sur les H^2 .

Considérons alors le diagramme commutatif :

$$\begin{array}{ccc} H^2(G,A_n) & \longrightarrow & H^2(G,A_{n'}) \\ \downarrow \inf & & \downarrow \inf \\ H^2(\bar{G},A_n) & \longrightarrow & H^2(\bar{G},A_{n'}) \end{array} .$$

Il est clair que l'image de ε_n par la première ligne est $\varepsilon_{n'}$. La nullité de $\inf \varepsilon_n$ entraîne donc celle de $\inf \varepsilon_{n'}$, ce qui se traduit (I. th. 1) en disant que si (P_n) admet une solution, $(P_{n'})$ aussi .

Si n'/n est impair et si n est une puissance de 2 , A_n est facteur direct de $A_{n'}$: il existe un sous-G-module M de $A_{n'}$ tel que :

$$A_{n'} = M \oplus A_n .$$

On a alors une décomposition des groupes de cohomologie :

$$H^2(G,A_{n'}) = H^2(G,M) \oplus H^2(G,A_n)$$
$$H^2(\bar{G},A_{n'}) = H^2(\bar{G},M) \oplus H^2(\bar{G},A_n) .$$

Dans la première décomposition, d'après la nullité du groupe $H^2(G,M)$ (G étant d'ordre 2 et M d'ordre impair) on a : $\varepsilon_{n'} = 0 \oplus \varepsilon_n$. Ce qui donne : $\inf \varepsilon_{n'} = 0 \oplus \inf \varepsilon_n$. Ainsi $\inf \varepsilon_n$ et $\inf \varepsilon_{n'}$ sont nuls en même temps, d'où la deuxième partie du théorème.

On sait que l'on peut se limiter aux valeurs paires de n . Les para-

graphes suivants vont être consacrés à la démonstration du théorème 2 :

Théorème 2.

Pour que (P_n) admette une solution, il faut que toute place réelle de k se prolonge dans $K = k(\sqrt{\alpha})$ en des places réelles. Cette condition étant supposée réalisée, (P_2) admet une solution si, et seulement si, (-1) est une norme de K/k, (P_4) admet une solution si, et seulement si, toute place v de k au-dessus de 2 telle que α soit dans $-(k_v)^2$ a un degré local pair sur le corps des rationnels. Pour que (P_8) admette une solution (c'est le cas si K et $\mathbb{Q}(\zeta)$ ne sont pas linéairement disjoints) il suffit qu'il existe une place v (divisant forcément 2α) telle qu'aucun des nombres 2, $-\alpha$, -2α ne soit dans $(k_v)^2$.

III.2. Etude de la condition sur les places infinies.

Soit v une place infinie de k, il s'agit de dire quand la condition locale nécessaire, relative à v est remplie. Si G_v est trivial le théorème 4 de I permet de conclure. Si G_v n'est pas trivial, on a à étudier (cf. I,4. remarque) la nullité de $\inf \varepsilon_v$ dans $H^2(\bar{G}_v, A)$. Or, on a la suite d'applications :

$$H^2(G,A) \xrightarrow[\sim]{\text{res}} H^2(G_v,A) \xrightarrow[\sim]{\text{inf}} H^2(\bar{G}_v,A) \quad .$$

Ces applications sont des isomorphismes, les groupes G_v et $\bar{G}_v$ étant en fait égaux à G. Ainsi $\inf \varepsilon_v$ est l'image de ε par un isomorphisme donc n'est pas nul : pour que la condition locale en v soit remplie, il faut et il suffit que G_v soit trivial.

En considérant toutes les places infinies de k, on obtient donc la condition nécessaire suivante, qui est celle du théorème :

"pour que (P_n) admette une solution, il faut que toute place réelle de k se prolonge en des places réelles de K".

III.3. Places modérément ramifiées dans K/k .

Soit v une place ramifiée dans K/k ne divisant pas 2 . Une telle place est non ramifiée dans $k(\zeta)/k$. Les extensions $k_v(\zeta)$ et K_v sont donc linéairement disjointes sur k_v . Dans Γ'_v , il existe donc un élément $\tilde{\tau}$ opérant non trivialement sur k_v et trivialement sur les racines $n^{\text{ièmes}}$ de l'unité. Un caractère invariant par Γ'_v doit être invariant par $\tilde{\tau}$. On a donc pour tout a de A_n :

$$\chi(a) = (\tilde{\tau}\chi)(a) = \chi^{-1}(a) \qquad \text{i.e.} \quad \chi(a) = \pm 1$$

$\wedge_{v,\chi}$ se factorise donc par l'application :

$$H^2(G_v, A) \xrightarrow{\chi} H^2(G_v, K_v^*) .$$

Cette application s'étudie à l'aide des $\hat{H}^\circ$:

$$\{1, \sigma^{n/2}\} = A^{G_v} \to k_v^*/NK_v^* .$$

Mais, on a $\chi(\sigma) = \pm 1$ d'où $\chi(\sigma^{n/2}) = +1$ dès que 4 divise n . Ce qui prouve que $\wedge_{v,\chi}$ est nul dès que 4 divise n . Ainsi, sauf peut être pour (P_2) dont l'étude est faite au paragraphe suivant, les conditions locales pour les places finies modérément ramifiées de K/k , sont automatiquement vérifiées.

III.4. Etude pour (P_2) .

En remarquant que E_2 est alors cyclique d'ordre 4 , on voit que l'on peut appliquer II théorème 1 qui nous dit qu'une condition nécessaire et suffisante pour que (P_2) admette une solution est que (-1) soit une norme locale pour toutes les places, donc une norme globale de K/k . Ceci justifie la partie du théorème 2 relative à (P_2) .

III.5. Etude pour (P_4) .

On commence par examiner l'injectivité de h , celle-ci étant acquise, (P_4) se réduit à l'étude des conditions locales ; cette étude est d'ailleurs déjà faite pour les places ne divisant pas 2 (en III.2 et III.3).

a) Injectivité de h .

Si $K(\zeta)/k$ est de degré 2 , Γ' est cyclique, donc Γ aussi et h est injective. Supposant $K(\zeta)$ de degré 4 sur k , $K(\zeta) = K' = k(\sqrt{-1},\sqrt{\alpha})$, on voit facilement que L est égal à $k(\sqrt{-\alpha})$ donc est cyclique de degré 2 sur k , ce qui prouve encore l'injectivité de h .

b) Etude des conditions locales pour les places au-dessus de 2 .

On distinguera trois cas :

1) $\alpha \notin \pm(k_v)^2$.

Ainsi K'_v/k_v est de degré 2 ou 4 . Il existe un élément $\tilde{\tau}$ de son groupe de Galois, laissant $\zeta = \sqrt{-1}$ invariant, mais pas α . Un caractère invariant par $\tilde{\tau}$ doit vérifier pour tout a de A_n :

$$\chi(a) = (\tilde{\tau}\chi)(a) = \chi^{-1}(a) .$$

D'où $\chi(a) = \pm 1$.

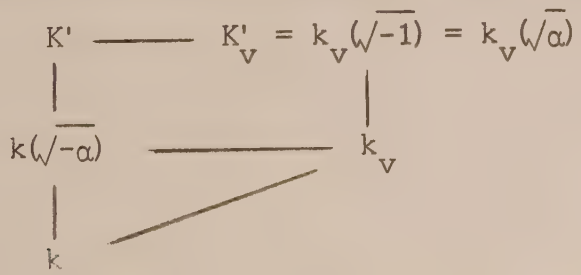
Le même raisonnement que celui de III.3. montre que la condition locale est remplie.

2) $\alpha \in k_v^2$.

G_v est alors trivial, les conditions locales sont vérifiées.

3) $\alpha \in -k_v^2$, $\alpha \notin k_v^2$.

On peut faire le schéma suivant, représentant des extensions de k et leurs complétés :



Comme Γ'_v agit par symétrie sur les racines de l'unité et sur A_4, il est clair que tous les caractères sont invariants. Etudions $\wedge_{v,\chi}$:

$$H^2(G,A) \xrightarrow{\sim} H^2(G_v,A) \xrightarrow{\sim} H^2(\Gamma'_v,A) \longrightarrow H^2(\Gamma'_v,K'_v) \quad .$$

Comme Γ'_v est cyclique, on passe en dimension 0 :

$$\{1,\sigma^2\} = \hat{H}^0(\Gamma'_v,A) \to k_v^*/NK_v'^* = \hat{H}^0(\Gamma'_v,K'_v) \quad .$$

Ainsi $\wedge_{v,\chi}$ est nul si, et seulement si, $\chi(\sigma^2)$ est une norme pour le caractère χ. Or, $\chi(\sigma^2)$ vaut +1 ou -1. D'autre part, K'_v s'obtient en rajoutant $\sqrt{-1}$ à k_v. La condition locale est donc vérifiée si, et seulement si, le symbole de Hilbert $(-1,-1)_{k_v}$ vaut 1, c'est-à-dire si le degré absolu de k_v est pair.

c) Conclusion.

Comme h est injective, les conditions locales sont nécessaires et suffisantes. Or, elles sont vérifiées, sauf peut-être pour les places finies au-dessus de 2, étudiées ci-dessus. Le théorème 2 est donc démontré pour la partie concernant (P_4).

III.6. Etude pour (P_8).

Etudions d'abord les cas où K et $\mathbb{Q}(\zeta)$ ne sont pas linéairement disjoints (a et b) :

a) $K = k(\sqrt{-1})$.

On observe que le corps L est égal à $k(\sqrt{2})$ donc est cyclique de degré 1 ou 2 sur k. L'application h est donc injective. Les conditions locales au-dessus de 2 sont donc nécessaires et suffisantes. Supposons d'abord que v soit telle que $\sqrt{2}$ ne soit pas dans k_v. Il existe alors dans Γ'_v un élément t opérant de la façon suivante sur les racines de l'unité :

$$\zeta^t = \zeta^5 \quad .$$

Ainsi $\sqrt{-1}$ est invariant, donc t n'opère pas sur A . L'action sur les caractères est donc : $\chi^t = \chi^5$. Tout caractère invariant par Γ'_v a donc son image dans $\{\pm 1, \pm\sqrt{-1}\}$ donc dans K_v^* . L'application $\wedge_{v,\chi}$ se factorise alors :

$$H^2(G,A) \longrightarrow H^2(G_v,A) \longrightarrow H^2(G_v,K_v^*) \xrightarrow{\inf} H^2(\Gamma'_v,K_v'^*) \quad .$$

L'application du milieu est nulle, car correspond en dimension 0 à :

$$A^{G_v} \xrightarrow{\chi} k_v^*/NK_v^* \quad .$$

Si G_v est nul le dernier groupe est nul et c'est évident. Si G_v n'est pas nul, on a : $A^{G_v} = \{1,\sigma^4\}$ et $\chi(\sigma^4) = \chi^4(\sigma) = 1$ d'où la nullité de l'application considérée.

Supposons maintenant que $\sqrt{2}$ soit dans k_v . Tous les caractères sont invariants ; la situation ressemble à celle de III.5.b)3), mais comme $\sqrt{2}$ est dans k_v le degré local est pair et la condition locale est remplie.

On voit donc que les conditions locales relatives à (P_8) sont toujours remplies, ce qui compte-tenu de l'injectivité de h signifie que (P_8) admet toujours une solution dans notre cas.

Remarque :

Puisque l'on suppose que la condition sur les places réelles est vérifiée, k désigne ici un corps de nombres totalement imaginaire.

b) Autres cas où K et $\mathbb{Q}(\zeta)$ ne sont pas linéairement disjoints.

Les sous-extensions quadratiques de $\mathbb{Q}(\zeta)$ étant engendrées par $\sqrt{2}$, $\sqrt{-2}$, $\sqrt{-1}$ les seuls cas possibles restants sont les suivants :

- $\sqrt{2} \in k$ ou $\sqrt{-2} \in k$ ou $\sqrt{-1} \in k$. Le degré local pour les places au-dessus de 2 est pair, donc les conditions locales pour (P_4) sont remplies ; (P_4) admettant une solution, d'après le théorème 1 il en est de même pour (P_8) .

- $K = k(\sqrt{2})$ ou $K = k(\sqrt{-2})$. Soit $\alpha = \pm 2$ si $\alpha \in -(k_v)^2$ alors k_v contient $\mathbb{Q}_2(\sqrt{2})$ ou $\mathbb{Q}_2(\sqrt{-2})$ et le degré local est pair. Les condi-

tions locales sont donc remplies : (P_4) et donc (P_8) admettent toujours une solution .

c) Cas où K et $\mathbb{Q}(\zeta)$ sont linéairement disjoints.

On va voir que dans ce cas h n'est pas forcément injective et que les conditions locales pour les places finies sont toujours toutes vérifiées. L'injectivité de h fournit donc une condition suffisante pour que (P_8) admette une solution : c'est celle du théorème 2.

1) Injectivité de h .

K et $\mathbb{Q}(\zeta)$ étant linéairement disjoints, Γ est engendré par trois générateurs d'ordre 2 :

- τ : laissant invariant les racines de l'unité, $\tau(\sqrt{\alpha}) = -\sqrt{\alpha}$.
- s tel que $s(\sqrt{\alpha}) = \sqrt{\alpha}$ et $s(\zeta) = \zeta^{-1}$.
- t tel que $t(\sqrt{\alpha}) = \sqrt{\alpha}$ et $t(\zeta) = \zeta^5$.

Ainsi pour tout caractère χ on a $\tau\chi = \chi^{-1} = s\chi$ et $t\chi = \chi^5$. Il est facile de voir que le groupe laissant fixe les caractères est $\{1, s\tau\}$. Le corps qui lui est associé est $L = k(\sqrt{2}, \sqrt{-\alpha})$.

On applique alors le théorème 2 du chapitre I : pour que h soit injective, il faut et il suffit qu'il existe une place v telle que $\Gamma_v = \Gamma$. Il est clair qu'une telle place est ramifiée. Dire que Γ est égal à Γ_v revient à dire qu'aucun des trois nombres 2 , $-\alpha$, -2α n'est dans $(k_v)^2$.

2) Vérification des conditions locales.

On peut supposer v au-dessus de 2 . On peut alors distinguer trois cas :

- $\Gamma'_v = \{1\}$
- $\Gamma'_v = \{1, s\tau\}$
- $\Gamma'_v \subsetneq \{1, s\tau\}$.

Dans le premier cas, il est clair que les applications $\wedge_{v,\chi}$ sont nulles pour χ dans $\hat{A}_v$. Dans le second cas, on observe que le raisonnement ressemble à celui de III.5.b)3) , le degré local étant pair, car $\sqrt{2}$, invariant par $s\tau$, est dans k_v . Dans le troisième cas, on observe qu'il existe des caractères non invariants. On a donc $\hat{A}_v \neq \hat{A}$. Le groupe $\hat{A}$ étant cyclique d'ordre 8 , on en déduit que les caractères dans $\hat{A}_v$ vérifient $\chi^4 = 1$, le raisonnement se termine alors comme celui de III.6.a).

III.7. Cas où le corps k est celui des rationnels.

Traduisons le théorème 2 dans le cas où K/k est une extension quadratique $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$. On choisit m entier sans facteur carré. La condition sur la place réelle signifie que m doit être positif. La condition sur (P_4) signifie que $(-m)$ ne doit pas être un carré de $\mathbb{Q}_2$, ce qui s'exprime encore en disant que m ne doit pas être congru à -1 mod 8 .

Pour (P_8) on voit que l'on peut supposer m congru à -1 modulo 8 (car sinon (P_4) admet déjà une solution). Si v est la place correspondant à 2 , $(-m)$ est donc alors dans $(k_v)^2$. Une place vérifiant la condition du théorème 2 correspondant donc à un diviseur premier p impair de m . Il est alors impossible que $-m$ et $-2m$ soient dans $(k_v)^2$. Tout revient donc à la non trivialité du symbole de Legendre

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} .$$

La condition suffisante est donc remplie lorsque m possède un facteur premier congru à ± 3 modulo 8 .

On peut donc retrouver les premiers résultats de [5] :

Théorème 3.

Pour que l'extension $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ (m entier sans facteur carré) se plonge dans une surextension quaternionienne sur $\mathbb{Q}$, il faut que m soit positif. Cette condition étant supposée réalisée, (P_2) admet une solution si et seule-

ment si m est somme de deux carrés de $\mathbb{Z}$, (P_4) admet une solution si et seulement si m est non congru à (-1) modulo 8, (P_8) admet une solution si m possède un facteur premier congru à ± 3 modulo 8.

En fait comme le dit [5] la réciproque pour (P_8) est vérifiée.
[5] donne aussi une condition suffisante pour que (P_n) admette une solution.

CHAPITRE IV

PLONGEMENT DANS UNE SUREXTENSION DE DEGRE p^3

IV.1. Introduction.

Soient p un nombre premier et K/k une extension galoisienne de type (p,p) de corps de nombres. Soit E le groupe d'ordre p^3 à deux générateurs σ et τ vérifiant les relations :

$$\sigma^{p^2} = 1$$

$$\tau^p = 1$$

$$\tau\sigma\tau^{-1} = \sigma^{1+p} \quad .$$

L'élément σ^p engendre un sous-groupe distingué A d'ordre p. Le quotient est engendré par les images $\bar{\sigma}$ et $\bar{\tau}$ de σ et τ ; on peut donc l'identifier non canoniquement au groupe de Galois G de K/k. On désigne par H le sous-groupe engendré par $\bar{\tau}$.

Le but de ce chapitre est d'étudier le problème du plongement ainsi défini. On conserve les notations du chap. I. Dans les cinq premiers paragraphes on suppose p impair.

IV.2. Examen des données.

a) Le groupe E.

Enonçons d'abord le lemme suivant dont la démonstration par récurrence à l'aide des formules définissant le groupe E est facile :

Lemme 1.

En désignant par r et s deux entiers, la puissance $q^{ième}$ de l'élément $\sigma^r\tau^s$ est de la forme $\sigma^{r_q}\tau^{q.s}$ avec :

$$r_q = r.q \quad (1 + s\frac{p(q-1)}{2}) \quad .$$

En particulier : $(\sigma^r\tau^s)^p = \sigma^{r.p}$ et $(\sigma^r\tau^s)^{1+p} = \sigma^{r(1+p)}\tau^s$.

D'après sa définition le groupe est extension de A par G . La structure correspondante de G-module sur A est triviale. L'extension est représentée par un élément ε de $H^2(G,A)$. La proposition suivante, qui prouve en particulier que cette extension est non décomposée, sera utile dans la suite :

Proposition 1.

Le sous-groupe H est le seul sous-groupe propre de G tel que la restriction de ε soit nulle.

Démonstration :

H est le seul sous-groupe de G dont l'image réciproque dans E soit de type (p,p) . La proposition en résulte en interprétant la restriction de ε en termes d'extensions.

b) Propriétés arithmétiques de k .

La proposition 2 met en évidence certaines propriétés de k découlant de l'existence d'une surextension de type (p,p) :

Proposition 2.

Si v est une place finie première à p , ramifiée dans K/k telle que G_v soit d'ordre p , alors k_v contient les racines $p^{ièmes}$ de l'unité. Si v est une place finie première à p ramifiée dans K/k telle que G_v soit d'ordre p^2 alors la ramification ne peut être totale (avec les notations usuelles on aura $e = f = p$, $g = 1$) k_v contient les racines de l'unité d'ordre p et K_v celles d'ordre p^2 .

Démonstration :

L'appartenance des racines $p^{\text{ièmes}}$ de l'unité à k_v provient dans tous les cas de [3] chap.I, §8, prop.1. Cette proposition nous dit aussi que toute extension totalement et modérément ramifiée est cyclique ; d'après la structure de G, l'indice de ramification d'une place première à p ne peut être p^2 : si G_v est d'ordre p^2 on aura $e = f = p$, $g = 1$. Observons que si U désigne le groupe des unités de k_v, U/U^p est d'ordre p (cf [3], chap.VI, §1.7 prop.5). Ainsi k_v ne possède qu'une extension cyclique non ramifiée de degré p ; c'est donc celle engendrée par les racines de l'unité d'ordre p^2, si celles-ci ne sont pas dans k_v. Ceci prouve que si G_v est d'ordre p^2, K_v contient les racines d'ordre p^2, ce qui achève de démontrer la proposition 2.

IV.3. Localisation de la condition de plongement.

a) Justification de la méthode.

Avec les notations du chapitre I, on voit que G opère trivialement sur A Γ' opère donc sur $\hat{A}$ par action galoisienne sur les racines de l'unité : on a donc $L = k(\zeta)$. Ce corps est cyclique sur k, on peut donc appliquer les théorèmes 2 et 3 du chap.I :

Théorème 1.

Le problème du plongement admet une solution si et seulement si les conditions locales sont toutes vérifiées.

Ce sont ces conditions locales que nous allons maintenant étudier.

b) Places pour lesquelles G_v est d'ordre p .

Proposition 3.

Si v est une place de k telle que G_v soit d'ordre p, la condition locale relative à v est vérifiée sauf si on a simultanément :

$$G_v \neq H \ , \ \zeta \in k_v \ , \ \zeta \notin N_{K_v/k_v}(K_v) \ .$$

Démonstration :

Pour chaque caractère χ invariant par Γ'_v on doit étudier la nullité de l'image $\wedge_{v,\chi}(\varepsilon)$ de ε par l'application :

$$H^2(G,A) \xrightarrow{\text{res}} H^2(G_v,A) \xrightarrow{\text{inf}} H^2(\Gamma'_v,A) \xrightarrow{\chi} H^2(\Gamma'_v,K'^*_v) \quad .$$

Mais dire qu'il existe un caractère invariant non trivial revient à dire que φ est dans k_v ; l'application $\wedge_{v,\chi}$ se factorise alors :

$$\begin{array}{ccccc} H^2(G,A) & \xrightarrow{\text{res}} & H^2(G_v,A) & \longrightarrow & H^2(G_v,K^*_v) \\ & & \downarrow \text{inf} & & \downarrow \text{inf} \\ & & H^2(\Gamma'_v,A) & \longrightarrow & H^2(\Gamma'_v,K'^*_v) \end{array} \quad .$$

Comme la dernière ligne est injective, il suffit de regarder l'image de ε par la première ligne, c'est-à-dire l'image de res ε par :

$$H^2(G_v,A) \to H^2(G_v,K^*_v) \quad .$$

On va étudier cette application en passant en dimension 0 . Si res ε est non nul (i.e. si G_v est distinct de H d'après prop. 1) l'élément qui lui correspond dans $\hat{H}^\circ(G_v,A)$ est non nul donc son image par

$$A = \hat{H}^\circ(G_v,A) \xrightarrow{\chi} \hat{H}^\circ(G,K^*_v) = k^*_v/NK^*_v$$

est nulle, χ n'étant pas trivial, que si ζ est une norme de K^*_v dans k^*_v . Ainsi pour que la condition locale ne soit pas vérifiée il faut et il suffit que G_v soit distinct de H , ζ étant dans k^*_v mais non dans NK^*_v .

c) Places premières à p pour lesquelles G_v est d'ordre p^2 .

Le résultat est donné par la proposition :

Proposition 4.

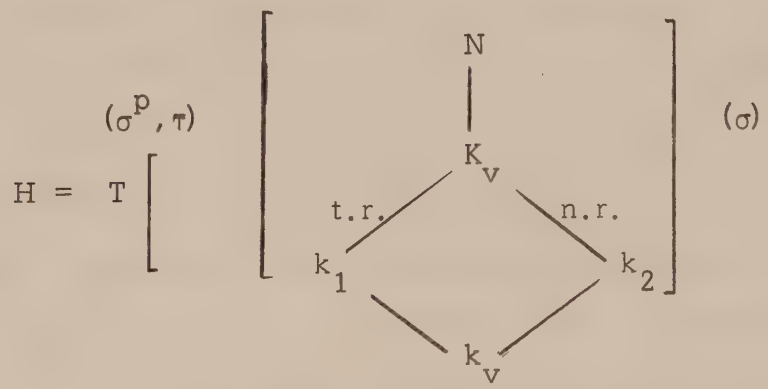
Si la place v première à p est telle que G_v soit d'ordre p^2 , la condition locale est remplie si et seulement si le prolongement continu de $\bar{\tau}$ à K^*_v (que l'on notera encore $\bar{\tau}$) opère sur les racines de l'unité d'ordre p^2 par élévation à la puissance $1+p$.

Démonstration :

Soit ε_v la restriction de ε dans $H^2(G_v,A)$. La condition locale revient à dire que inf ε_v inflation de ε_v dans $H^2(\overline{G}_v,A)$ est nulle. Or ceci revient à dire (cf. remarque finale de chap.I) que le problème de plongement relatif à K_v/k_v et à E considéré comme extension de A par G_v (ici $G = G_v$) admet une solution. C'est sous cette forme que nous allons voir si la condition locale est remplie. Introduisons les notations suivantes : k_1 et k_2 désignent les sous extensions de K_v/k_v correspondant respectivement à $\overline{\pi}$ et $\overline{\sigma}$. Soit T le groupe d'inertie de v dans K_v/k_v ; T est d'ordre p (prop. 2).

1°) Supposons d'abord que le problème de plongement local admette une solution N .

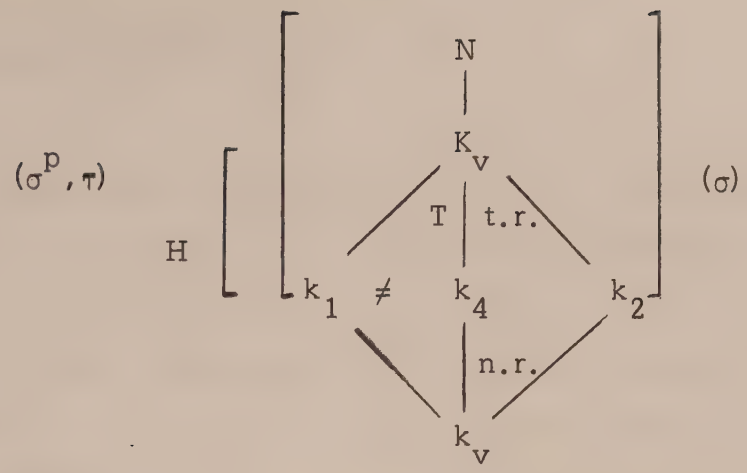
- Si les sous-groupes T et H sont égaux on peut faire le diagramme suivant :



▪ Si N/K_v est totalement ramifiée, N/k_1 est totalement et modérément ramifiée donc cyclique ce qui est absurde.

▪ Si N/K_v est non ramifiée, l'indice de ramification de N/k_v est p . Soit donc k_3 la sous-extension non ramifiée maximale. Les extensions k_3 et k_2 sont linéairement disjointes sur k_v et engendrent donc N . Le groupe de Galois de N/k_v est le produit de ceux de k_2/k_v et k_3/k_v il est donc abélien ce qui est absurde. On voit donc ainsi que T et H ne peuvent être égaux.

- Soit donc k_4 la sous-extension non ramifiée maximale de K_v/k_v on a alors le schéma :



Si l'extension N/K_v était non ramifiée, il en serait de même de N/k_1 qui serait donc cyclique ce qui est absurde. Ainsi N/k_4 est totalement et modérément ramifiée, on peut appliquer [3] chap.I, §8, prop.1 : k_4 contient les racines de l'unité d'ordre p^2 (cf. aussi 2.2. prop.2, ci-dessus), N/k_4 étant une extension de Kummer : il existe un élément γ de k_4 tel que $N = k_4(\sqrt[p^2]{\gamma})$. En plus k_4 correspond à un sous-groupe a de E engendré par un élément de la forme $\sigma\tau^\lambda$ ($\lambda \in Z$) , le quotient g étant engendré par l'image $\tilde{\tau}$ de τ . Le groupe g opère sur a par

$$\tilde{\tau}(\sigma\tau^\lambda) = \tau\sigma\tau^\lambda\tau^{-1} = \sigma^{1+p}\tau^\lambda = (\sigma\tau^\lambda)^{1+p}$$

(cf. §2.1, lemme). Supposons que $\tilde{\tau}$ opère sur les racines de l'unité d'ordre p^2 par : $\zeta_{p^2} \to \zeta_{p^2}^{1+rp}$. Soit χ le caractère de a associé par la théorie de Kummer à γ , on sait qu'à $\tilde{\tau}(\gamma)$ correspondra le caractère $\tilde{\tau}(\chi)$:

$$\tilde{\tau}(\chi) = \chi^{(1+rp)(1-p)} = \chi^{1+(r-1)p}$$

($\tilde{\tau}(\chi)$ est déduit de χ en faisant agir $\tilde{\tau}$ sur les racines de l'unité et $\tilde{\tau}^{-1}$ sur a). Ainsi $\tilde{\tau}(\gamma)$ et $\gamma^{1+(r-1)p}$ seront associés au même caractère :

$$\tilde{\tau}\gamma = \gamma^{1+(r-1)p} \quad \text{dans} \quad k_4^* \text{ modulo } (k_4^*)^{p^2} \quad .$$

En comparant les valuations des deux nombres on obtient :

$$v(\gamma)\ (r-1)p \equiv 0 \quad \text{modulo } p^2 \ .$$

Ainsi si r est distinct de 1 modulo p, la valuation de γ est divisible par p ce qui est absurde puisque N/k_4 est totalement ramifiée. Ainsi : si le problème de plongement local si possible, les racines de l'unité sont envoyées par $\tilde{\tau}$ sur

leur puissance $(1+p)^{\text{ième}}$.

2°) Montrons que réciproquement si $\bar{\tau}$ opère sur les racines de l'unité d'ordre p^2 par $\zeta_{p^2} \to \zeta_{p^2}^{1+p}$ le problème de plongement local admet une solution. D'après nos hypothèses et la proposition 2, k_v contient les racines $p^{\text{ièmes}}$ de l'unité ; l'extension k_1 est donc engendré par $\sqrt[p]{\gamma}$ racine $p^{\text{ième}}$ d'un élément γ de k_v . De plus, d'après l'action de τ sur les racines d'ordre p^2 celles-ci ne sont pas toutes dans k_1 , de sorte que si ζ_{p^2} est une racine primitive on a $K_v = k_v(\zeta_{p^2}, \sqrt[p]{\gamma})$. On voit alors facilement que $N = k_v(\zeta_{p^2}, \sqrt[p^2]{\gamma})$ est une solution au problème de plongement. En effet, il est clair que N est galoisien sur k_v . De plus son groupe de Galois est engendré par deux éléments s et t définis par leur action sur ζ_{p^2} et $\sqrt[p^2]{\gamma}$:

$$s(\sqrt[p^2]{\gamma}) = \zeta_{p^2}\sqrt[p^2]{\gamma} \qquad s(\zeta_{p^2}) = \zeta_{p^2}$$

$$t(\sqrt[p^2]{\gamma}) = \sqrt[p^2]{\gamma} \qquad t(\zeta_{p^2}) = \zeta_{p^2}^{1+p}$$

On vérifie alors facilement les formules :

$$s^{p^2} = 1 \qquad t^p = 1 \qquad tst^{-1} = s^{1+p} \quad .$$

Soient $\bar{s}$ et $\bar{t}$ les restrictions de s et t à K_v . On a :

$$\bar{\tau} = \bar{t}$$

$$\bar{\sigma} = \bar{s}^{\lambda}\bar{t}^{\mu} \quad \text{avec} \quad \lambda \in \{1,\ldots,p-1\} \quad \mu \in \{0,\ldots,p-1\} \quad .$$

Posons alors : $\sigma_1 = s^{\lambda}t^{\mu}$, $\tau_1 = t$ on obtient les relations (d'après les relations sur s et t et le lemme 1 du §2) :

$$\sigma_1^{p^2} = 1 \qquad \tau_1^p = 1 \qquad \tau_1\sigma_1\tau_1^{-1} = \sigma_1^{1+p} \quad .$$

Ceci prouve que le groupe de Galois de N/k_v est isomorphe à E . Cet isomorphisme fait correspondre le groupe de Galois de N/K_v et A ainsi que le groupe de Galois de K_v/k_v et G . Le problème de plongement local admet donc N comme solution.

IV.4. "Oubli" d'une place.

Au §3 on n'a pas traité le cas des places v divisant p telles que G_v soit d'ordre p^2. Or on va voir dans la suite que dans l'examen des conditions locales on peut dans certaines conditions oublier une place.

a) Adjonction des racines $p^{\text{ièmes}}$ de l'unité.

Pour discuter l'oubli d'une place, il faut adjoindre (cf. 4.b) les racines $p^{\text{ièmes}}$ de l'unité. Soient donc $K' = K(\zeta)$, $k' = k(\zeta)$. Les propositions suivantes expriment le lien entre les problèmes de plongement pour K/k et K'/k'.

Proposition 5.

Si le problème de plongement admet une solution pour K/k, il en est de même pour K'/k' et réciproquement.

Démonstration :

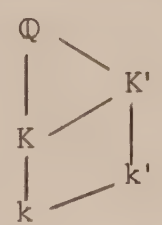
Soient $\overline{G}$, $\overline{G}'$ et G' les groupes de Galois des extensions $\overline{\mathbb{Q}}/k$, $\overline{\mathbb{Q}}/k'$, K'/k'. On rappelle que pour que le problème de plongement pour K/k admette une solution, il faut et il suffit que l'image de $\mathfrak{e}$ par l'inflation suivante soit nulle :

$$H^2(G,A) \to H^2(\overline{G},A) .$$

On a un résultat analogue pour K'/k'. Le diagramme commutatif suivant relie les groupes de Galois :

$$\begin{array}{ccc} \overline{G}' & \to & \overline{G} \\ \downarrow & & \downarrow \\ G' & \xrightarrow{\sim} & G \end{array}$$

correspondant à



.

La première ligne est l'injection naturelle, la seconde l'isomorphisme de restriction entre G' et G. Les colonnes sont les homomorphismes canoniques. On en déduit le diagramme :

$$\begin{array}{ccc} H^2(G,A) & \xrightarrow{\text{inf}} & H^2(\overline{G},A) \\ \downarrow\mathfrak{s} & & \downarrow \text{res} \\ H^2(G',A) & \xrightarrow{\text{inf}} & H^2(\overline{G}',A) \end{array} .$$

Comme $\overline{G}/\overline{G}'$ est un groupe fini d'ordre premier à celui de A, la restriction est injective. L'image de ε par la première colonne est ε' ; la possibilité du plongement pour K/k est liée à la nullité de $\inf \varepsilon$ et pour K'/k' à celle de $\inf \varepsilon'$. Le diagramme précédent montre que ces nullités sont équivalentes d'où la proposition 5.

Proposition 6.

Soit v une place de k, v' un prolongement quelconque à k', les conditions locales en v et v' pour K/k et K'/k' sont équivalentes.

Démonstration :

On rappelle qu'on a choisi un prolongement, encore noté v, de v à $\overline{\mathbb{Q}}$. Faisons de même pour v'. Avec des notations évidentes on a le diagramme suivant entre les groupes de décomposition :

$$\begin{array}{ccccc} \overline{G}'_{v'} & \xrightarrow{\sim} & \overline{G}'_{v} & \to & \overline{G}_{v} \\ \downarrow & & \downarrow & & \downarrow \\ G'_{v'} & \xrightarrow{\sim} & G'_{v} & \xrightarrow{\sim} & G_{v} \end{array} .$$

Les isomorphismes des lignes sont des conjugaisons. Les colonnes sont définies par les homomorphismes canoniques. Le dernier carré est l'équivalent de celui de la proposition 6 mais appliqué aux groupes de décomposition. On déduit de ce diagramme, le diagramme suivant :

$$\begin{array}{ccccc} H^2(G_v,A) & \xrightarrow{\sim} & H^2(G'_v,A) & \xrightarrow{\sim} & H^2(G'_{v'},A) \\ \downarrow \inf & & \downarrow \inf & & \downarrow \inf \\ H^2(\overline{G}_v,A) & \xrightarrow{\text{res}} & H^2(\overline{G}'_v,A) & \xrightarrow{\sim} & H^2(\overline{G}'_{v'},A) \end{array} .$$

Soient ε_v et $\varepsilon'_{v'}$ les restrictions de ε et de ε' à G_v et $G'_{v'}$. Les conditions locales sont équivalentes à la nullité de $\inf \varepsilon_v$ et $\inf \varepsilon'_{v'}$. Or la restriction de la deuxième ligne étant injective (même raisonnement que pour la proposition 6) ces nullités sont équivalentes d'où la proposition 6.

b) Oubli d'une place de k' .

Proposition 7.

Si toutes les conditions locales sauf peut être une sont vérifiées pour K'/k' , elles sont toutes vérifiées.

Démonstration :

Supposons que toutes les conditions locales soient vérifiées pour K'/k' sauf peut-être celle relative à une place v'_o . Considérons alors le diagramme suivant associé à chaque caractère χ de A :

$$\begin{array}{ccccc} H^2(\bar{G}',A) & \to & \sum_{v'} H^2(\bar{G}'_{v'},A) & & \\ \downarrow \chi & & \downarrow \chi & & \\ 0 \to H^2(\bar{G}',\bar{\Phi}^*) & \to & \sum_{v'} H^2(\bar{G}_{v'},k'_{v'}) & \xrightarrow{\Sigma \text{ inv}} & \Phi/\mathbb{Z} \end{array} .$$

La première ligne est définie par le produit des restrictions de $\bar{G}'$ à $G'_{v'}$ lorsque v' décrit l'ensemble de toutes les places de k' . La deuxième ligne est la suite exacte classique (cf. [3], chap. VIII, §11) . Observons que la condition locale pour une place v' est équivalente à la nullité de $\chi(\inf \varepsilon'_{v'})$ pour tous les caractères de A invariants, donc ici pour tous les caractères de A . Or $\chi(\inf \varepsilon'_{v'})$ provient par restriction de l'élément $\chi(\inf \varepsilon')$ de $H^2(\bar{G}',\bar{\Phi}^*)$ dont la somme des invariants est nulle. Ainsi la nullité pour chaque χ des $\chi(\inf \varepsilon'_{v'})$ pour toute place v' distincte de v'_o entraîne celle des $\chi(\inf \varepsilon'_{v'})$ pour toutes les places de k' . D'où la proposition.

IV.5. Récapitulation de l'étude $(p \neq 2)$.

Les résultats précédents permettent d'énoncer :

Théorème 2.

Soit K/k une extension galoisienne de type (p,p) de corps de nombres. On suppose qu'il existe au plus une place v'_o de $k' = k(\zeta)$ au-dessus de p non décomposée dans K'/k'. Alors, pour que le problème de plongement relatif à E ait une solution il faut et il suffit que les conditions locales soient vérifiées pour toutes les places v de k :

v	condition locale
$G_v = \{1\}$	toujours vérifiée
$G_v = H$	toujours vérifiée
G_v d'ordre p $G_v \neq H$	$\zeta \notin k_v^*$ ou $\zeta \in N_{K_v/k_v}(K_v^*)$
G_v d'ordre p^2 $p \nmid v$ $\Downarrow$ $\zeta \in k_v$ et $\zeta_{p^2} \in K_v$	Le prolongement de $\bar{\tau}$ à K_v opère sur ζ_{p^2} par élévation à la puissance $(1+p)$
G_v d'ordre p^2 $p \mid v$ $\Downarrow$ v = restriction de v'_o	conséquence des conditions précédentes

■ Remarque : Le théorème s'applique en particulier lorsque k est égal à $\mathbb{Q}$ ou à $\mathbb{Q}(\zeta)$.

IV.6. Etude pour $p = 2$. Comparaison avec [4] .

Le groupe E s'appelle alors le groupe diédral . Ses propriétés ne rentrent pas tout à fait dans le cas général :

Proposition 8.

Le seul sous-groupe propre de G tel que la restriction de ε soit non nulle est $\{1,\bar{\sigma}\}$.

Le problème de plongement se traite comme dans les paragraphes précédents : le théorème 1 est encore valable mais les propositions 3 et 4 doivent être adaptées.

Proposition 9.

Si v est une place de k telle que G_v soit d'ordre 2 la condition relative à v est vérifiée sauf si on a simultanément :

$$G_v = \{1,\bar{\sigma}\} \quad \text{et} \quad -1 \notin N_{K_v/k_v}(K_v^*) \quad .$$

Démonstration : cf. prop.3 en remplaçant la prop.1 par la prop.8.

Soient α et β deux éléments de k tels que $k(\sqrt{\alpha})$, $k(\sqrt{\beta})$ et $k(\sqrt{\alpha\beta})$ soient les trois sous-extensions de K correspondant respectivement aux sous-groupes $\{1,\bar{\sigma}\}$, $\{1,\bar{\tau}\}$, $\{1,\overline{\sigma\tau}\}$.

Proposition 10.

Si la place v , première à 2, est telle que G_v soit d'ordre 4 la condition locale est remplie si et seulement si $(-\alpha)$ est un carré de k_v .

Démonstration :

On procède comme dans la démonstration de la proposition 4. On en reprend les notations. On trouve que pour que la condition locale soit vérifiée, c'est-à-dire pour que le problème de plongement local admette une solution, il faut que (-1) ne soit pas carré dans $k_1 = k_v(\sqrt{\beta})$. L'extension N est alors cyclique sur k_4 et seulement sur k_4 . Comme $k_4 = k_v(\sqrt{-1})$ on doit avoir $k_v(\sqrt{\alpha}) = k_v(\sqrt{-1})$ donc $(-\alpha)$ doit être un carré de k_v .

La réciproque se fait comme dans la proposition 4 : si $(-\alpha)$ est un carré de k_v , (-1) n'est pas carré de $k_v(\sqrt{\beta})$ on a $K_v = k_v(\sqrt{-1},\sqrt{\beta})$. L'extension $N = k_v(\sqrt{-1},\sqrt[4]{\beta})$ est galoisienne de groupe isomorphe à E sur k_v et cyclique sur $k_v(\sqrt{-1}) = k_v(\sqrt{\alpha})$ elle répond donc au problème de plongement local.

Une extension N/k est dite diédrale, si elle est galoisienne, de groupe de Galois isomorphe à E . Le résultat suivant généralise [4] et [7] :

Théorème 3.

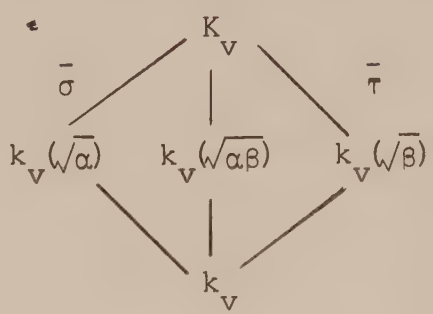
Soient α et β deux éléments de k tels que $K = k(\sqrt{\alpha}, \sqrt{\beta})$ soit de degré 4 . On suppose qu'il existe au plus une place v_o de k au-dessus de 2 et non décomposée dans K/k . Pour que K/k se plonge dans une surextension diédrale sur k et cyclique sur $k(\sqrt{\alpha})$ il faut et il suffit que β soit norme d'un élément de $k(\sqrt{-\alpha})$.

Démonstration :

Pour que β soit une norme de $k(\sqrt{-\alpha})$ il faut et il suffit que ce soit une norme locale. Pour chaque place v de k on doit donc avoir la relation suivante sur le symbole de Hilbert :

$$(-\alpha, \beta)_v = 1 \ .$$

On va comparer cette condition (sauf peut être en v_o) à la condition locale du problème du plongement (cf. Prop.9 et prop.10) :



- $G_v = \{1\}$. Les deux conditions locales sont vérifiées en v .
- $G_v = \{1, \bar{\tau}\}$, β est alors carré de k_v d'où $(-\alpha, \beta)_v = 1$. Les deux conditions locales en v sont vérifiées.
- $G_v = \{1, \bar{\sigma}\bar{\tau}\}$, $\alpha\beta$ est alors carré de k_v d'où $(-\alpha, \alpha\beta)_v = 1$ d'où à l'aide de $(-\alpha, \alpha)_v = 1$, $(-\alpha, \beta)_v = 1$. Les deux conditions locales en v sont vérifiées.
- $G_v = \{1, \bar{\sigma}\}$, α est carré de k_v , de là :

  $$(-\alpha, \beta)_v = 1 \Leftrightarrow (-1, \beta)_v = 1 \Leftrightarrow -1 \in N_{K_v/k_v}(K_v^*) \ .$$

  Les deux conditions locales en v sont donc équivalentes.
- $G_v = \{1, \bar{\sigma}, \bar{\tau}, \bar{\sigma}\bar{\tau}\}$.

- si $(-\alpha)$ est carré de k_v on a $(-\alpha,\beta)_v = 1$. Ainsi la condition locale de la prop. 10 entraîne celle du théorème 3.

- réciproquement, supposons que $(-\alpha,\beta)_v = 1$. Calculons le symbole de Hilbert grâce à [17] XIV, §3, prop.8 :

  . 1er cas : $v(\alpha)$ est pair et $v(\beta)$ impair ; la condition signifie que $(-\alpha)$ est carré de k_v .

  . 2e cas : $v(\alpha)$ est impair et $v(\beta)$ pair ; la condition signifie que β est carré de k_v , ce qui est absurde puisque G_v est d'ordre 4.

  . 3e cas : $v(\alpha)$ et $v(\beta)$ sont impairs $(\alpha\beta)$ est alors un carré de k_v ce qui est aussi absurde.

Ainsi si G_v est d'ordre 4 les conditions de la prop. 10 et du théorème 3 sont équivalentes.

-o00o-

BIBLIOGRAPHIE

[1] - ADACHI - "On the imbedding problem of Galois extensions". J. Math. Soc. Japan, vol. 22 (1970).

[2] - ARTIN-TATE - "Class field theory".

[3] - CASSELS-FROHLICH - "Algebraic Number theory".

[4] - DAMEY-PAYAN - "Existence et construction des extensions galoisiennes et non abéliennes de degré 8 d'un corps de caractéristiques différente de 2". J.f.d.r.u.a. Math 244.

[5] - DAMEY - "Sur certaines 2-extensions galoisiennes non abéliennes d'un corps de caractéristique différente de 2". Thèse Grenoble 1971.

[6] - GILLARD - "Sur le problème du plongement des extensions galoisiennes". C.R.A.S. t. 274, p. 1436. Série A.

[7] - HALTER-KOCH - "Arithmetische theorie der Normalkorper von 2-Potenzgrad mit Diedergruppe". Journal of Number theory, vol.3, n°4.

[8] - HOECHSMANN - "Zum Einbettungsproblem". J.f.d.r.u.a. Math. 229.

[9] - KERKOUR-AHMED - "Construction d'extensions cycliques dont le degré est une puissance d'un nombre premier impair". Thèse 3e cycle, Besançon.

[10] - PAYAN - "Critère de décomposition d'une extension de Kummer sur un sous-corps du corps de base". Ann. Scient. Ec. Norm. Sup. 4e série t.1.

[11] - POITOU - "Cohomologie galoisienne des modules finis".

.../...

[12] - REICHARDT - "Konstruction von Zahlkörpern mit gegebener Galois Gruppe von Primzahlpotenzordnung". J.f.d.r.u.a. Math. 177.

[13] - RICHTER - "Über die Lösbarkeit des Einbettungsproblems für abelsche Zahlkörper". Math. Annalen, n° 112.

[14] - ŠAFAREVIČ - "Construction of fields of algebraic numbers with given solvable Galois groups". traduit dans Ann. Math. Soc. Translations (2), 4.

[15] - ŠAFAREVIČ - "On the problem of imbedding fields". traduit dans Ann. Math. Soc. Translations (2), 4.

[16] - SERRE - "Cours d'arithmétique".

[17] - SERRE - "Corps locaux".

[18] - SERRE - "Cohomologie galoisienne".

[19] - SONN - "On the embedding problem for nonsolvable groups of Algebraic Number fields : reduction theorems". Journ. of Number theory, n°4.

-o00o-

LISTE DES PROFESSEURS

Président : Monsieur Michel SOUTIF
Vice-Président : Monsieur Gabriel CAU

PROFESSEURS TITULAIRES

MM.	ANGLES D'AURIAC Paul	Mécanique des fluides
	ARNAUD Georges	Clinique des maladies infectieuses
	ARNAUD Paul	Chimie
	AUBERT Guy	Physique
	AYANT Yves	Physique approfondie
Mme	BARBIER Marie-Jeanne	Electrochimie
MM.	BARBIER Jean-Claude	Physique expérimentale
	BARBIER Reynold	Géologie appliquée
	BARJON Robert	Physique nucléaire
	BARNOUD Fernand	Biosynthèse de la cellulose
	BARRA Jean-René	Statistiques
	BARRIE Joseph	Clinique chirurgicale
	BENOIT Jean	Radioélectricité
	BERNARD Alain	Mathématiques Pures
	BESSON Jean	Electrochimie
	BEZES Henri	Chirurgie générale
	BLAMBERT Maurice	Mathématiques Pures
	BOLLIET Louis	Informatique (IUT B)
	BONNET Georges	Electrotechnique
	BONNET Jean-Louis	Clinique ophtalmologique
	BONNET-EYMARD Joseph	Pathologie médicale
	BONNIER Etienne	Electrochimie Electrométallurgie
	BOUCHERLE André	Chimie et Toxicologie
	BOUCHEZ Robert	Physique nucléaire
	BOUSSARD Jean-Claude	Mathématiques Appliquées
	BRAVARD Yves	Géographie
	BRISSONNEAU Pierre	Physique du Solide
	BUYLE-BODIN Maurice	Electronique
	CABANAC Jean	Pathologie chirurgicale
	CABANEL Guy	Clinique rhumatologique et hydrologie
	CALAS François	Anatomie
	CARRAZ Gilbert	Biologie animale et pharmacodynamie
	CAU Gabriel	Médecine légale et Toxicologie
	CAUQUIS Georges	Chimie organique
	CHABAUTY Claude	Mathématiques Pures
	CHARACHON Robert	Oto-Rhino-Laryngologie
	CHATEAU Robert	Thérapeutique
	CHENE Marcel	Chimie papetière
	COEUR André	Pharmacie chimique
	CONTAMIN Robert	Clinique gynécologique
	COUDERC Pierre	Anatomie Pathologique
	CRAYA Antoine	Mécanique
Mme	DEBELMAS Anne-Marie	Matière médicale
MM.	DEBELMAS Jacques	Géologie générale
	DEGRANGE Charles	Zoologie
	DESRE Pierre	Métallurgie
	DESSAUX Georges	Physiologie animale
	DODU Jacques	Mécanique appliquée
	DOLIQUE Jean-Michel	Physique des plasmas
	DREYFUS Bernard	Thermodynamique
	DUCROS Pierre	Cristallographie
	DUGOIS Pierre	Clinique de Dermatologie et Syphiligraphie
	FAU René	Clinique neuro-psychiatrique
	FELICI Noël	Electrostatique
	GAGNAIRE Didier	Chimie physique
	GALLISSOT François	Mathématiques Pures
	GALVANI Octave	Mathématiques Pures
	GASTINEL Noël	Analyse numérique
	GEINDRE Michel	Electroradiologie
	GERBER Robert	Mathématiques Pures
	GIRAUD Pierre	Géologie
	KLEIN Joseph	Mathématiques Pures
Mme	KOFLER Lucie	Botanique et Physiologie végétale
MM.	KOSZUL Jean-Louis	Mathématiques Pures
	KRAVTCHENKO Julien	Mécanique
	KUNTZMANN Jean	Mathématiques Appliquées
	LACAZE Albert	Thermodynamique
	LACHARME Jean	Biologie végétale
	LAJZEROWICZ Joseph	Physique
	LATREILLE René	Chirurgie générale
	LATURAZE Jean	Biochimie pharmaceutique
	LAURENT Pierre	Mathématiques Appliquées
	LEDRU Jean	Clinique médicale B
	LLIBOUTRY Louis	Géophysique
	LOUP Jean	Géographie
Mlle	LUTZ Elisabeth	Mathématiques Pures
	MALGRANGE Bernard	Mathématiques Pures
	MALINAS Yves	Clinique obstétricale
	MARTIN-NOEL Pierre	Sémiologie médicale
	MASSEPORT Jean	Géographie
	MAZARE Yves	Clinique médicale A
	MICHEL Robert	Minéralogie et Pétrographie
	MOURIQUAND Claude	Histologie
	MOUSSA André	Chimie nucléaire
	NEEL Louis	Physique du Solide
	OZENDA Paul	Botanique
	PAUTHENET René	Electrotechnique
	PAYAN Jean-Jacques	Mathématiques Pures
	PEBAY-PEYROULA Jean-Claude	Physique
	PERRET René	Servomécanismes
	PILLET Emile	Physique Industrielle
	RASSAT André	Chimie systématique
	RENARD Michel	Thermodynamique
	REULOS René	Physique industrielle
	RINALDI Renaud	Physique
	ROGET Jean	Clinique de pédiatrie et de puériculture
	SANTON Lucien	Mécanique
	SEIGNEURIN Raymond	Microbiologie et Hygiène
	SENGEL Philippe	Zoologie
	SILBERT Robert	Mécanique des fluides
	SOUTIF Michel	Physique générale
	TANCHE Maurice	Physiologie
	TRAYNARD Philippe	Chimie générale
	VAILLAND François	Zoologie
	VALENTIN Jacques	Physique Nucléaire
	VAUQUOIS Bernard	Calcul électronique
Mme	VERAIN Alice	Pharmacie galénique
M.	VERAIN André	Physique
Mme	VEYRET Germaine	Géographie
MM.	VEYRET Paul	Géographie
	VIGNAIS Pierre	Biochimie médicale
	YOCCOZ Jean	Physique nucléaire théorique

PROFESSEURS ASSOCIES

MM.	BULLEMER Bernhard	Physique

PROFESSEURS SANS CHAIRE

MM.	BEAUDOING André	Pédiatrie
Mme	BERTRANDIAS Françoise	Mathématiques Pures
MM.	BERTRANDIAS Jean-Paul	Mathématiques appliquées
	BIAREZ Jean-Pierre	Mécanique
	BONNETAIN Lucien	Chimie minérale
Mme	BONNIER Jane	Chimie générale
MM.	CARLIER Georges	Biologie végétale
	DEPASSEL Roger	Mécanique des Fluides
	DEPORTES Charles	Chimie minérale
	GAUTHIER Yves	Sciences biologiques
	GAVEND Michel	Pharmacologie
	GERMAIN Jean Pierre	Mécanique
	GIDON Paul	Géologie et Minéralogie
	GLENAT René	Chimie organique
	HACQUES Gérard	Calcul numérique
	JANIN Bernard	Géographie
Mme	KAHANE Josette	Physique
MM.	MULLER Jean-Michel	Thérapeutique
	PERRIAUX Jean-Jacques	Géologie et minéralogie
	POULOUJADOFF Michel	Electrotechnique
	REBECQ Jacques	Biologie (CUS)
	REVOL Michel	Urologie
	REYMOND Jean-Charles	Chirurgie générale
	ROBERT André	Chimie papetière
	DE ROUGEMONT Jacques	Neurochirurgie
	SARRAZIN Roger	Anatomie et chirurgie
	SARROT-REYNAULD Jean	Géologie
	SIBILLE Robert	Construction Mécanique
	SIROT Louis	Chirurgie générale
Mme	SOUTIF Jeanne	Physique générale

MAITRES DE CONFERENCES ET MAITRES DE CONFERENCES AGREGES

Mlle	AGNIUS-DELORD Claudine	Physique pharmaceutique
	ALARY Josette	Chimie analytique
MM.	AMBLARD Pierre	Dermatologie
	AMBROISE-THOMAS Pierre	Parasitologie
	ARMAND Yves	Chimie
	BEGUIN Claude	Chimie organique
	BELORIZKY Elie	Physique
	BENZAKEN Claude	Mathématiques Appliquées
	BILLET Jean	Géographie
	BLIMAN Samuel	Electronique (EIE)
	BLOCH Daniel	Electrotechnique
Mme	BOUCHE Liane	Mathématiques (CUS)
MM.	BOUCHET Yves	Anatomie
	BOUVARD Maurice	Mécanique des Fluides
	BRODEAU François	Mathématiques (IUT B)
	BRUGEL Lucien	Energétique
	BUISSON Roger	Physique
	BUTEL Jean	Orthopédie
	CHAMBAZ Edmond	Biochimie médicale
	CHAMPETIER Jean	Anatomie et organogénèse
	CHIAVERINA Jean	Biologie appliquée (EFP)
	CHIBON Pierre	Biologie animale
	COHEN-ADDAD Jean-Pierre	Spectrométrie physique
	COLOMB Maurice	Biochimie médicale
	CONTE René	Physique
	COULOMB Max	Radiologie
	CROUZET Guy	Radiologie
	DURAND Francis	Métallurgie
	DUSSAUD René	Mathématiques (CUS)
Mme	ETERRADOSSI Jacqueline	Physiologie
MM.	FAURE Jacques	Médecine légale
	GENSAC Pierre	Botanique
	GIDON Maurice	Géologie
	GRIFFITHS Michaël	Mathématiques Appliquées
	GROULADE Joseph	Biochimie médicale
	HOLLARD Daniel	Hématologie
	HUGONOT Robert	Hygiène et Médecine préventive
	IDELMAN Simon	Physiologie animale
	IVANES Marcel	Electricité
	JALBERT Pierre	Histologie
	JOLY Jean-René	Mathématiques Pures
	JOUBERT Jean-Claude	Physique du Solide
	JULLIEN Pierre	Mathématiques Pures
	KAHANE André	Physique générale
	KUHN Gérard	Physique
	LACOUME Jean-Louis	Physique
Mme	LAJZEROWICZ Jeannine	Physique
MM.	LANCIA Roland	Physique atomique
	LE JUNTER Noël	Electronique
	LEROY Philippe	Mathématiques
	LOISEAUX Jean-Marie	Physique Nucléaire
	LONGEQUEUE Jean-Pierre	Physique Nucléaire
	LUU DUC Cuong	Chimie Organique
	MACHE Régis	Physiologie végétale
	MAGNIN Robert	Hygiène et Médecine préventive
	MARECHAL Jean	Mécanique
	MARTIN-BOUYER Michel	Chimie (CUS)
	MAYNARD Roger	Physique du Solide
	MICHOULIER Jean	Physique (I.U.T. "A")
	MICOUD Max	Maladies Infectieuses
	MOREAU René	Hydraulique (INP)
	NEGRE Robert	Mécanique
	PARAMELLE Bernard	Pneumologie
	PECCOUD François	Analyse (IUT B)
	PEFFEN René	Métallurgie
	PELMONT Jean	Physiologie animale
	PERRET Jean	Neurologie
	PERRIN Louis	Pathologie expérimentale
	PFISTER Jean-Claude	Physique du Solide
	PHELIP Xavier	Rhumatologie
Mlle	PIERY Yvette	Biologie animale
MM.	RACHAIL Michel	Médecine interne
	RACINET Claude	Gynécologie et obstétrique
	RENAUD Maurice	Chimie
	RICHARD Lucien	Botanique
Mme	RINAUDO Marguerite	Chimie macromoléculaire
MM.	ROMIER Guy	Mathématiques (IUT B)
	SHOM Jean Claude	Chimie Générale
	STIEGLITZ Paul	Anesthésiologie
	STOEBNER Pierre	Anatomie pathologique
	VAN CUTSEM Bernard	Mathématiques Appliquées
	VEILLON Gérard	Mathématiques Appliquées (INP)
	VIALON Pierre	Géologie
	VOOG Robert	Médecine interne
	VROUSSOS Constantin	Radiologie
	ZADWORNY François	Electronique

MAITRES DE CONFERENCES ASSOCIES

MM.	BOUDOURIS Georges	Radioélectricité
	CHEEKE John	Thermodynamique
	YACOUD Mahmoud	Médecine légale

CHARGES DE FONCTIONS DE MAITRES DE CONFERENCES

Mme	BERIEL Hélène	Physiologie

Fait le 30 Mai 1972

VU,

Grenoble, le

Le Président de la thèse,

C. CHABAUTY

VU, et permis d'imprimer

Grenoble, le

Le Président de l'Université scientifique
et médicale,

M. SOUTIF